6

566.39530X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: M. KAYASHIMA, et al

Serial No.: 09/761,742

Filing Date: January 18, 2001

For: SECURITY MANAGEMENT SYSTEM AND METHOD THEREFOR

Art Unit: Not yet assigned

LETTER CLAIMING RIGHT OF PRIORITY

Assistant Commissioner
for Patents
Washington, D.C. 20231

May 18, 2001

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, applicants hereby claim the right of priority based on:

Japanese Application No. 2000-012123
Filed: January 20, 2000

Japanese Application No. 2000-270186
Filed: September 6, 2000

Certified copies of said application documents are attached hereto.

Respectfully submitted,

Carl I. Brundidge
Registration No. 29,621
ANTONELLI, TERRY, STOUT & KRAUS, LLP

CIB/jdc
Enclosures
703/312-6600

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２０日

出願番号
Application Number: 特願２０００－０１２１２３

出願人
Applicant (s): 株式会社日立製作所

２００１年　２月１６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２００１－３００８３９７

【書類名】　特許願

【整理番号】　HL12821000

【提出日】　平成12年 1月20日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/24

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　寺田　真敏

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　萱島　信

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　礒川　弘実

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　永井　康彦

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区戸塚町５０３０番地　株式会社日立製作所　ソフトウェア事業部内

【氏名】　加藤　恵理

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100087170

【弁理士】

【氏名又は名称】　富田　和子

【電話番号】　045(316)3711

【手数料の表示】

【予納台帳番号】　012014

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】セキュリティ管理システム

【特許請求の範囲】

【請求項１】

情報システムを構成する複数の被管理対象システムのセキュリティーの状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するセキュリティ管理システムであって、

少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティの状態を、当該対応する情報セキュリティポリシーに整合するように制御する複数の管理手段と、

情報セキュリティポリシー、被管理対象システムおよび管理手段の対応を登録した対応管理データベースと、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付手段と、

前記対応管理データベースにおいて、前記セキュリティ内容受付手段が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている管理手段を抽出する抽出手段と、

前記抽出手段が抽出した管理手段に、当該管理手段に対応する被管理対象システムのセキュリティの状態を、当該管理手段に対応する情報セキュリティポリシーに整合するように変更させる管理制御手段と、を有すること

を特徴とするセキュリティ管理システム。

【請求項２】

情報システムを構成する複数の被管理対象システムの、セキュリティ施策のポリシーを表す情報セキュリティポリシーに関わるセキュリティーの状態を監査するセキュリティ管理システムであって、

少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査する、複数の監査手段と、

情報セキュリティポリシー、被管理対象システムおよび監査手段との対応を登

録した対応管理データベースと、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付手段と、

前記対応管理データベースにおいて、前記セキュリティ内容受付手段が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている監査手段を抽出する抽出手段と、

前記抽出手段が抽出した監査手段に、当該監査手段に対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査させる監査制御手段と、を有すること

を特徴とするセキュリティ管理システム。

【請求項３】

情報システムを構成する複数の被管理対象システムのセキュリティーの状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するセキュリティ管理システムであって、

少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティの状態を、当該対応する情報セキュリティポリシーに整合するように制御する、複数の管理手段と、

少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査する、複数の監査手段と、

情報セキュリティポリシー、被管理対象システム、管理手段および監査手段の対応を登録した対応管理データベースと、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付手段と、

前記対応管理データベースにおいて、前記セキュリティ内容受付手段が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている管理手段と監査手段を抽出する抽出手段と、

前記抽出手段が抽出した管理手段に、当該管理手段に対応する被管理対象システムのセキュリティの状態を、当該管理手段に対応する情報セキュリティポリシ

ーに整合するように変更させる管理制御手段と、

前記抽出手段が抽出した監査手段に、当該監査手段に対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査させる監査制御手段と、を有すること

を特徴とするセキュリティ管理システム。

【請求項４】

情報システムを構成する複数の被管理対象システムのセキュリティーの状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するセキュリティ管理方法であって、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるステップと、

予め記憶された、少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティの状態を当該対応する情報セキュリティポリシーに整合するように制御する処理が記述された複数の管理プログラムから、選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応する管理プログラムを抽出するステップと、

抽出した管理プログラムを実行させ、当該管理プログラムに対応する被管理対象システムのセキュリティの状態を、当該管理プログラムに対応する情報セキュリティポリシーに整合するように変更させるステップと、を有すること

を特徴とするセキュリティ管理方法。

【請求項５】

情報システムを構成する複数の被管理対象システムの、セキュリティ施策のポリシーを表す情報セキュリティポリシーに関わるセキュリティーの状態を監査するセキュリティ管理方法であって、

ユーザより、情報セキュリティポリシーと被管理対象システムの範囲の選択を受け付けるステップと、

予め記憶された、少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキ

ユリティポリシーに関わるセキュリティの状態を監査する処理が記述された複数の監査プログラムから、選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている監査プログラムを抽出するステップと、

抽出した監査プログラムを実行させ、当該監査プログラムに対応する被管理対象システムの当該監査プログラムに対応する情報セキュリティポリシーに関わるセキュリティの状態を監査させるステップと、を有すること

を特徴とするセキュリティ管理方法。

【請求項６】

情報システムを構成する複数の被管理対象システムのセキュリティーの状態を、セキュリティ施策のポリシーを表す情報セキュリティポリシーに従って制御するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読み取られて実行されることで、

ユーザより、情報セキュリティポリシーおよび被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付手段と、

少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキュリティの状態を当該対応する情報セキュリティポリシーに整合するように制御する処理が記述された複数の管理プログラムを格納するデータベースから、前記セキュリティ内容受付手段が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応する管理プログラムを抽出する抽出手段と、

前記抽出手段が抽出した管理プログラムを実行させ、当該管理プログラムに対応する被管理対象システムのセキュリティの状態を、当該管理プログラムに対応する情報セキュリティポリシーに整合するように変更させる管理制御手段とを、前記電子計算機上に構築すること

を特徴とするプログラムが記憶された記憶媒体。

【請求項７】

情報システムを構成する複数の被管理対象システムの、セキュリティ施策のポリシーを表す情報セキュリティポリシーに関わるセキュリティーの状態を監査す

るためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読み取られて実行されることで、

ユーザより、情報セキュリティポリシーと被管理対象システムの範囲の選択を受け付けるセキュリティ内容受付手段と、

少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査する処理が記述された複数の監査プログラムを格納するデータベースから、前記セキュリティ内容受付手段が選択を受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応して登録されている監査プログラムを抽出する抽出手段と、

前記抽出手段が抽出した監査プログラムを実行させ、当該監査プログラムに対応する被管理対象システムの当該監査プログラムに対応する情報セキュリティポリシーに関わるセキュリティの状態を監査させる監査制御手段とを、前記電子計算機上に構築すること

を特徴とするプログラムが記憶された記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークに接続した各種処理装置からなる情報処理システムの、セキュリティの状態の制御および管理を支援する技術に関する。

【０００２】

【従来の技術】

近年、インターネット技術等を用いた情報システムが企業活動のインフラとして広く活用されるようになったことに伴い、情報システムに対する不正アクセスやウィルスによる情報資産への脅威を回避するためのセキュリティシステムの重要性が一段と高まっている。

【０００３】

このようなセキュリティシステムを管理するための従来の技術としては、ファイアウォールやウィルス対策プログラムなどの、情報システム上の個々のセキュ

リティシステムの設定や変更を行うTivoli社の製品Tivoli Security Management などが知られている。

【０００４】

【発明が解決しようとする課題】

さて、情報システムのセキュリティ対策は、情報システム全体の脅威分析に基づく対策方針である情報セキュリティポリシーの作成、情報セキュリティポリシーに従った情報システムのセキュリティシステムの導入および運用管理といった一連の手順を経て実施することが望まれている。このような手順に沿った情報システムのセキュリティ対策を推奨するものとしては、1999年6月にISO15408として国際標準化されたセキュリティ評価基準CC(Common Criteria)がある。

【０００５】

しかしながら、上記従来の技術によれば、情報セキュリティポリシーに従ったセキュリティ対策を実現するために導入したセキュリティシステムが何であるのかや、各情報セキュリティポリシーに対してセキュリティシステムをどのように運用管理しているのかなどを管理するための仕組みがない。

【０００６】

このため、情報セキュリティポリシーに従った情報システムのセキュリティの状態の制御や管理は、情報セキュリティポリシーならびにセキュリティシステムに関する高度な専門知識を有する管理者でなければ、行うことが困難であった。また、情報セキュリティポリシーに従った情報システムのセキュリティの状態の制御や管理に要する時間やコストなどの負担が大きかった。

【０００７】

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、情報セキュリティポリシーに従った、情報システムのセキュリティの状態の制御や管理を簡単にすることにある。

【０００８】

【課題を解決するための手段】

上記目的達成のために、本発明は、少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムのセキ

ュリティの状態を、当該対応する情報セキュリティポリシーに整合するように制御する複数の管理手段を用意する。そして、ユーザより受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応する管理手段を抽出して、当該管理手段に、当該管理手段に対応する被管理対象システムのセキュリティの状態を、当該管理手段に対応する情報セキュリティポリシーに整合するように変更させる。

【０００９】

また、本発明は、少なくとも１つの被管理対象システムおよび情報セキュリティポリシーに対応し、当該対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査する複数の監査手段を用意する。そして、ユーザより受け付けた範囲に含まれる情報セキュリティポリシーおよび被管理対象システムに対応する監査手段を抽出して、当該監査手段に、当該監査手段に対応する被管理対象システムの当該対応する情報セキュリティポリシーに関わるセキュリティの状態を監査させる。

【００１０】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

【００１１】

図１に、本実施形態に係る情報システムの構成を示す。

【００１２】

図示するように、情報システムは、情報セキュリティポリシー管理・監査支援装置31と、サーバやルータやファイアウォールなどの管理・監査対象計算機32とが、ネットワーク33を介して接続された構成を有している。

【００１３】

図２に、情報セキュリティポリシー管理・監査支援装置31の構成を示す。

【００１４】

図示するように、情報セキュリティポリシー管理・監査支援装置31のハードウエア構成は、たとえば、ＣＰＵ11と、メモリ12と、ハードディスク装置などの外部記憶装置13と、ネットワーク33に接続された通信装置14と、キーボードやマウ

スなどの入力装置15と、ディスプレイなどの表示装置16と、ＦＤやＣＤ-ＲＯＭなどの可搬性を有する記憶媒体からデータを読み取る読取り装置17と、上述した各構成要素間のデータ送受信を司るインタフェース18とを備えた、一般的な電子計算機上に構築することができる。

【００１５】

ここで、外部記憶装置13上には、情報セキュリティポリシー管理・監査支援装置31の各機能を電子計算機上に構築するための支援プログラム134が格納されている。ＣＰＵ11は、このプログラム134をメモリ12上にロードし実行することにより、管理・監査対象領域制御部111、情報セキュリティポリシー選択制御部112、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113、および、入出力制御部114を、電子計算機上に実現する。また、外部記憶装置１３上に、システム構成機器情報データベース131、情報セキュリティーデータベース132、および、セキュリティ管理・監査プログラムデータベース133を形成する。また、図示は省略したが、電子計算機上には、ネットワーク33を介して他装置と相互に通信するための通信制御部なども構築される。

【００１６】

図３に、管理・監査対象計算機３２の構成を示す。

【００１７】

ここで、図２に示す情報セキュリティポリシー管理・監査支援装置３１と同じ機能を有するものには同じ符号を付している。

【００１８】

図示するように、管理・監査対象計算機32の外部記憶装置13には、管理・監査対象計算機32上で稼動するＯＳプログラム150と、アプリケーションプログラム137と、アプリケーションプログラム137のセキュリティ管理・監査を行うセキュリティ管理・監査プログラム群136が格納されている。

【００１９】

ＣＰＵ11は、メモリ12上にロードされたＯＳプログラム１５０を実行することにより、ＯＳ151を電子計算機上に実現する。また、メモリ12上にロードされたアプリケーションプログラム137を実行することにより、サーバやルータやファ

イアウォールなどが有する個々のサービスを提供するアプリケーション部138を電子計算機上に実現する。また、メモリ12上にロードされたセキュリティ管理・監査プログラム群136に含まれる管理プログラムを実行することにより、ＯＳ151やアプリケーション部138のセキュリティ施策の状態を設定変更するセキュリティ管理部139を電子計算機上に実現し、セキュリティ管理・管理プログラム群136に含まれる監査プログラムを実行することにより、ＯＳ151やアプリケーション部138のセキュリティ施策の状態を確認するセキュリティ監査部140を電子計算機上に実現する。また、図示は省略したが、電子計算機上には、ネットワーク33を介して他装置と相互に通信するための通信制御部なども構築される。

【００２０】

次に、情報セキュリティポリシー管理・監査支援装置３１の各データベースについて説明する。

【００２１】

図４に、システムの構成機器情報データベース131の内容を示す。

【００２２】

図中、各行において、列41には、情報セキュリティポリシー管理・監査の対象となるシステムを一意に識別する識別子(SYSID)が記述される。列44には、列41のSYSIDで示されるシステムを構築するソフトウェアプログラム名（ＯＳプログラム150やアプリケーションプログラム137の名称）が記述される。列42には、列41のSYSIDで示されるシステムが稼働する装置の種別(例えば、ルータ、サーバ、クライアント、ファイアウォールなど)が記述される。そして、列45には、列41のSYSIDで示されるシステムの操作者による選択結果が格納される。

【００２３】

図５に、情報セキュリティポリシーデータベース132の内容を示す。

【００２４】

図中、各行において、列51には、情報セキュリティポリシーを一意に識別する識別子(POLICYID)が記述される。列52には、列51のPOLICYIDの欄に記述された情報セキュリティポリシーの施策種別(例えば、識別と認証、アクセス制御機能など)が記述される。列53には、列51のPOLICYIDの欄に記述された情報セキュリテ

ィポリシーの内容を表すセキュリティ施策(例えば、ネットワークにアクセス可能な端末の限定、識別・認証情報用の良いパスワード設定の実施など)が記述される。そして、列54には、列51のPOLICYIDで示される情報セキュリティポリシーの操作者による選択結果が格納される。

【００２５】

図６に、セキュリティ管理・監査プログラムデータベース133の内容を示す。

【００２６】

図中、各行において、列61には、情報セキュリティポリシーを一意に識別する識別子(POLICYID)が記述される。列62の管理プログラムの欄には、列61のPOLICYIDの欄に記述された情報セキュリティポリシーのセキュリティ施策の管理を行う管理プログラムの名称621と、名称621の管理プログラムが管理を行うシステムのSYSID623と、名称621の管理プログラムの実行要否を表す対応付け623が記述される。そして、列63の監査プログラムの欄には、列61のPOLICYIDの欄に記述された情報セキュリティポリシーのセキュリティ施策の監査を行う監査プログラムの名称631と、名称631の監査プログラムが監査を行うシステムのSYSID633と、名称631の監査プログラムの実行要否を表す対応付け633が記述される。

【００２７】

以下、このような情報システムにおける、セキュリティポリシー管理・監査の動作について説明する。

【００２８】

図７に、セキュリティポリシー管理・監査装置31の動作手順を示す。

【００２９】

まず、管理・監査対象領域制御部111は、入出力制御部114を用いて、表示装置16に、図８に示すような、外部記憶装置13上に形成されているシステム構成機器情報データベース131に登録されている内容を表した情報セキュリティポリシー管理・監査対象領域選択画面を表示する(ステップS701)。

【００３０】

図８において、「装置種別」91、「ソフトウェア種別」92および「プログラム名」93の各項目は、システム構成機器情報データベース131の列42、43、44に、

それぞれ対応している。この画面上で、操作者は、任意の項目91～93で情報セキュリティポリシー管理・監査対象領域を指定し、これを項目「使用可否」94のボタンで選択できる。この選択結果は、管理・監査対象領域制御部111によって、システム構成機器情報データベース131の列45に反映される。すなわち、ある装置種別が選択された場合にはその装置種別が記述された全ての行の列45に、また、あるソフトウェア種別が選択された場合にはそのソフトウエア種別が記述された全ての行の列４５に、さらにまた、あるプログラム名が選択された場合にはそのプログラム名が記述されたの行の列45に、選択可否として「YES」を登録する。

【００３１】

次に、操作者によって情報セキュリティポリシー管理・監査対象領域が選択されると、(ステップS702)、情報セキュリティポリシー選択制御部112は、入出力制御部114を用いて、表示装置16に、図９に示すような、情報セキュリティポリシーデータベース132に登録されている内容を表した情報セキュリティポリシー選択画面を表示する(ステップS703)。

【００３２】

図９において、「施策種別」1001および「セキュリティ施策」1002の各項目は、情報セキュリティポリシーデータベース１３２の列32、33に、それぞれ対応している。この画面上で、操作者は、任意の項目1001、1002で情報セキュリティポリシーを指定し、これを項目「使用可否」1003のボタンで選択できる。この選択結果は、情報セキュリティポリシー選択制御部112によって、情報セキュリティポリシーデータベース132の列54に反映される。すなわち、ある施策種別が選択された場合にはその施策種別が記述された全ての行の列54に、また、あるセキュリティ施策が選択された場合にはそのセキュリティ施策が記述された行の列54に、選択可否として「YES」を登録する。

【００３３】

次に、操作者によって情報セキュリティポリシーが選択されると(ステップS704)、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、ステップS701～S704により選択された結果に基づき、選択された情

報セキュリティポリシーとシステムに対応する管理・監査プログラムを、セキュリティ管理・監査プログラムデータベース133から抽出する。そして、抽出した管理・監査プログラムの対応付けの列623、633に「要」を登録する(ステップS705)。

【００３４】

この抽出は、図１０に示す手順によって行う。

【００３５】

すなわち、セキュリティ管理・監査プログラムデータベース133において、まず、情報セキュリティポリシーの検索を、列61を対象にステップS704で選択された(情報セキュリティポリシーデータベース132において列54に「YES」が登録されている）識別子(POLICYID)の有無を用いて行う(ステップS801)。次に、管理プログラムの抽出を、検索した識別子(POLICYID)と同じ行にある列622を対象に、ステップS702で選択されたシステム(システム構成機器情報データベース１３１において列54に「YES」が登録されている）の識別子(SYSID)の有無を用いて行う(ステップS803、S804)。それから、監査プログラムの抽出を、検索された識別子(POLICYID)と同じ行にある列632を対象に、ステップS702で選択されたシステム(システム構成機器情報データベース131において列「54」にYESが登録されている）の識別子(SYSID)の有無を用いて行う(ステップS804、S805)。

【００３６】

さて、図７に戻り、管理・監査プログラムの抽出が終わると、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、入出力制御部114を用いて、表示装置16に、図１１に示すような、情報セキュリティポリシーの実施状況ならびにセキュリティ施策の変更を指定するための画面を表示する(ステップS706)。

【００３７】

図１１において、「施策種別」1001および「セキュリティ施策」1002の各項目は、情報セキュリティポリシーデータベース132の列32、33に、それぞれ対応しており、ステップS704で選択された(YESが列54に設定された）もののみが表示される。操作者は、「施策種別」1001および「セキュリティ施策」1002の各項目に

おいて、管理や監査の対象となる情報セキュリティポリシーを１あるいは複数選択することができる。また、項目「管理」1101は、情報セキュリティポリシーの選択後、管理プログラムを用いて、選択した情報セキュリティポリシーに関わるセキュリティ施策の変更を行うためのボタンであり、項目「監査」1102は、情報セキュリティポリシーの選択後、監査プログラムを用いて、選択した情報セキュリティポリシーに関わる情報セキュリティポリシーの実施状況を確認するためのボタンである。操作者は、「管理」1101および「監査」1102のいずれかのボタンを選択できる。

【００３８】

さて、操作者により、情報セキュリティポリシーが選択され、そして、「管理」1101および「監査」1102のいずれかのボタンを選択されると(ステップS707)、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、ステップS705において、選択された情報セキュリティポリシーに対して抽出された（セキュリティ管理・監査プログラムデータベース133の対応付けの列623、624に「要」がマークされた）、セキュリティ管理プログラムあるいは監査プログラムを、ネットワーク33を介して起動する。

【００３９】

選択されたボタンが「管理」1101である場合、管理・監査対象計算機32上の管理・監査プログラム群136のうち、上記のようにして抽出された管理プログラムが起動され、実行される。管理プログラムの実行により具現化するセキュリティ管理部139は、管理・監査対象計算機32の表示装置16上に、たとえば図１２に示すような、セキュリティシステムの設定変更などの管理画面を表示する(ステップS708)。そして、セキュリティシステムの設定変更を受付て設定し、その内容をネットワーク33を介して情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答する。応答を受けた情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、その内容を情報セキュリティポリシー管理・監査支援装置31の表示装置16上に表示する。

【００４０】

なお、図１２は、図５に示す情報セキュリティポリシーデータベース132にお

いて、施策種別52「識別と認証機能」、セキュリティ施策53「識別・認証情報用の良いパスワード設定の実施」に対応する情報セキュリティポリシー「AUTH-01」を管理する管理プログラムである、パスワード管理プログラム（図６の管理プログラム名621「ADM_USR_#２」）が起動された場合の例を示している。図１２の画面は、パスワードの設定変更を受け付ける画面である。

【００４１】

一方、ステップS707において、選択されたボタンが「監査」1102である場合、管理・監査対象計算機32上の管理・監査プログラム群136のうち、上記のようにして抽出された監査プログラムが起動され、たとえば、図１３に示すような動作手順によって、その監査プログラムが監査を行うシステムのセキュリティ監査を行う(ステップS709)。そして、その結果を、ネットワーク33を介して、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答する。応答を受けた情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、その内容を情報セキュリティポリシー管理・監査支援装置31の表示装置16に表示する。

【００４２】

なお、図１３は、図５に示す情報セキュリティポリシーデータベース132において、施策種別52「アクセス監視」、セキュリティ施策53「データ・プログラムの改ざん検出の実施」に対応する情報セキュリティポリシー「ACCADM-01」を管理する監査プログラムである、データ改ざん監査プログラム（図６の管理プログラム名621「AUDIT_LOG_#１」）が起動あれた場合の例を示している。この例では、監査プログラムは、改竄検出プログラム自体が管理・監査対象計算機32上にインストールされ稼動されているか否かを確認し(ステップS1701)、次に、その稼動動作ログが保存されているかを確認する(ステップS1702)。それから、稼動動作ログの更新日を確認することで改ざん検出プログラムの継続稼動を確認する(ステップS1703)。そして、全ての確認項目に対して確認できたならば、監査結果は良好であるので、監査結果として「実施済」を情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答する(ステップS1705)。一方、そうでないならば、監査結果は不良となるので、監査結果として「実施

未」を情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113に応答するる(ステップS1704)。

【００４３】

さて、図７に戻り、情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部113は、監査結果の応答を受けとると、それを表示装置16に表示する(ステップS710)。

【００４４】

以上、本発明の実施形態について説明した。

【００４５】

ところで、以上では、図４のプログラム名44に記述されるプログラムを単位として、管理・監査プログラムを設けた場合について説明した。しかしながら本発明はこれに限定されない。たとえば、図４に示すシステムの構成機器情報データベース131において、装置種別42に記述される装置やソフトウエア種別43に記述されるソフトウエアを単位として、この単位毎に管理・監査プログラムを設け、選択された装置種別やソフトウエア種別とキュリティ施策に応じて、管理・監査プログラムを実行するようにしてもよい。

【００４６】

なお、装置種別を単位として、管理・監査プログラムを設ける場合、監査結果の表示は、たとえば、次のように行うことができる。

【００４７】

図１４は、監査結果を、図４に示すシステムの構成機器情報データベース131の装置種別42毎に、図５に示す情報セキュリティポリシーデータベースの施策種別52毎の、当該施策種別の全セキュリティ施策数53に対する実施済の割合を、いわゆるレーダーチャートを用いて表示する例を示している。また、図１５は、前記実施済の割合を表を用いて表示する例を示している。

【００４８】

図１４あるいは図１５において、操作者は、タグ1201を指定することで、装置種別42毎の監査結果を表示させることができる。また、操作者が、施策種別1202を指定し、ボタン「詳細」1203を選択したならば、図１７に示すような、図５に

示す情報セキュリティポリシーデータベースの施策種別52毎に、セキュリティ施策53毎の応答された監査結果を表示する。

【００４９】

図１７において、操作者は、監査結果に基づき、設定変更などの管理を実施したい場合や、再度、監査を実施したい場合、列1402の選択欄をチェックし、管理プログラムを用いてセキュリティ施策の変更を行うためのボタン「管理」1402、あるいは、監査プログラムを用いて情報セキュリティポリシーの実施状況の確認を行うためのボタン「監査」1403を選択することができる。

【００５０】

図１６は、監査結果を、図５に示す情報セキュリティポリシーデータベースの施策種別52毎に、図４に示すシステムの構成機器情報データベース131の装置種別42毎の、当該施策種別の全セキュリティ施策数53に対する実施済の割合を、いわゆるレーダーチャートを用いて表示する例を示している。

【００５１】

図１６において、操作者は、タグ1501を指定することで、施策種別52毎の監査結果を表示させることができる。また、操作者が、装置種別1502を指定し、ボタン「詳細」1503を選択したならば、図１７に示すような、図５に示す情報セキュリティポリシーデータベースの施策種別52毎に、セキュリティ施策53毎の応答された監査結果を表示する。

【００５２】

また、以上の実施形態では、管理・監査プログラムを管理・監査対象計算機３２上に配置したが、これらをネットワーク３３を介して管理・監査対象計算機３２上のシステムを管理・監査するプログラムとして構成し、これらを情報セキュリティーポリシー管理・監査支援装置３１上に配置するようにしてもよい。

【００５３】

また、以上の実施形態において、管理プログラムや監査プログラム自身が、パスワードの変更やログの収拾など、情報セキュリティポリシーに関わるその他の処理を実行するようにしてもよい。

【００５４】

さて、本実施形態によれば、以下のような効果がある。

【００５５】

（１）操作者が管理・監査対象となるシステムを指定し、情報セキュリティポリシーを選択するだけで、その構成で必要となるセキュリティ管理・監査プログラムが選択される。このため、情報セキュリティポリシーに従ったセキュリティ対策を実現するために導入したセキュリティシステムとの対応付けが容易となる。

【００５６】

（２）操作者が入力した情報セキュリティポリシーの管理実施を指定するだけで、その対象システムの情報セキュリティポリシーの適用を行う管理プログラムを起動することができる。このため、情報セキュリティポリシーに従った情報システムの運用管理を行うために、高度な専門知識を有しない管理者の場合にも、運用管理が容易となる。

【００５７】

（３）操作者が入力した情報セキュリティポリシーの状態を監査実施を指定するだけで、その対象システムの情報セキュリティポリシーに基づくセキュリティ施策の状態を評価することができる。このため、情報セキュリティポリシーに従った情報システムの運用管理状態を把握するために、高度な専門知識を有しない管理者の場合にも実施が容易となる。

【００５８】

【発明の効果】

以上のように、本発明によれば、情報セキュリティポリシーに従った、情報システムのセキュリティの状態の制御や管理を簡単にすることができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態が適用された情報システムの概略構成図である。

【図２】

図１に示す情報セキュリティポリシー管理・監査支援装置31の概略構成図である。

【図３】

図１に示す管理・監査対象計算機32の概略構成図である。

【図４】

図２に示すシステム構成機器情報データベース131の内容を説明するための図である。

【図５】

図２に示す情報セキュリティポリシーデータベース132の内容を説明するための図である。

【図６】

図２に示すセキュリティ管理・監査プログラムデータベース133の内容を説明するための図である。

【図７】

図１に示す情報セキュリティポリシー管理・監査支援装置31の動作手順を示すフロー図である。

【図８】

図７のステップS701で表示される、情報セキュリティポリシー管理・監査対象領域選択画面を示す図である。

【図９】

図７のステップS703で表示される、情報セキュリティポリシー選択画面を示す図である。

【図１０】

図７のステップS705における処理手順を示すフロー図である。

【図１１】

図７のステップS706で表示される、情報セキュリティポリシーの実施状況/セキュリティ施策の変更画面を示す図である。

【図１２】

管理プログラムが起動された場合の表示画面例を示す図である。

【図１３】

監査プログラムの起動された場合の処理手順例を示すフロー図である。

【図１４】

情報セキュリティポリシーの監査結果表示画面を示す図である。

【図１５】

情報セキュリティポリシーの監査結果表示画面を示す図である。

【図１６】

情報セキュリティポリシーの監査結果表示画面を示す図である。

【図１７】

情報セキュリティポリシーの監査結果表示画面を示す図である。

【符号の説明】

11…ＣＰＵ、31…情報セキュリティポリシー管理・監査支援装置

32…管理・監査対象計算機、33…ネットワーク

111…管理・監査対象領域制御部、112…情報セキュリティポリシー選択制御部

113…情報セキュリティポリシー/セキュリティ管理・監査プログラム関連付け制御部

114…入出力制御部、131…システムの構成機器情報データベース

132…情報セキュリティポリシーデータベース

133…セキュリティ管理・監査プログラムデータベース

134…情報セキュリティポリシー管理・監査支援プログラム

137…アプリケーションプログラム

136…セキュリティ管理・監査支援プログラム群

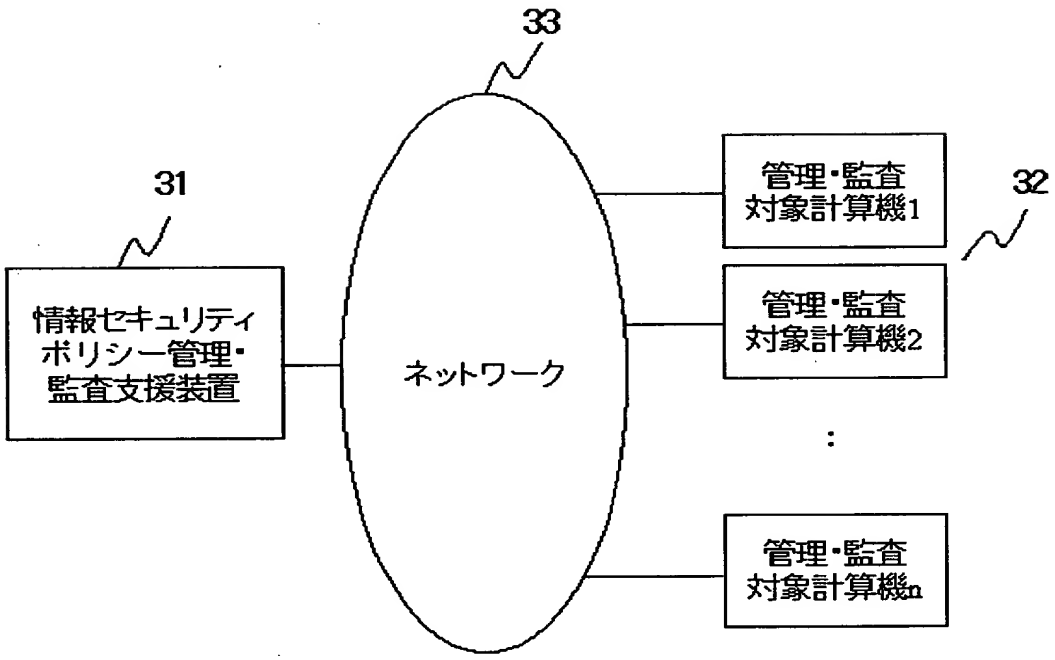
138…アプリケーション部、139…セキュリティ管理部

140…セキュリティ監査部、150…ＯＳプログラム、151…ＯＳ

【書類名】図面

【図１】

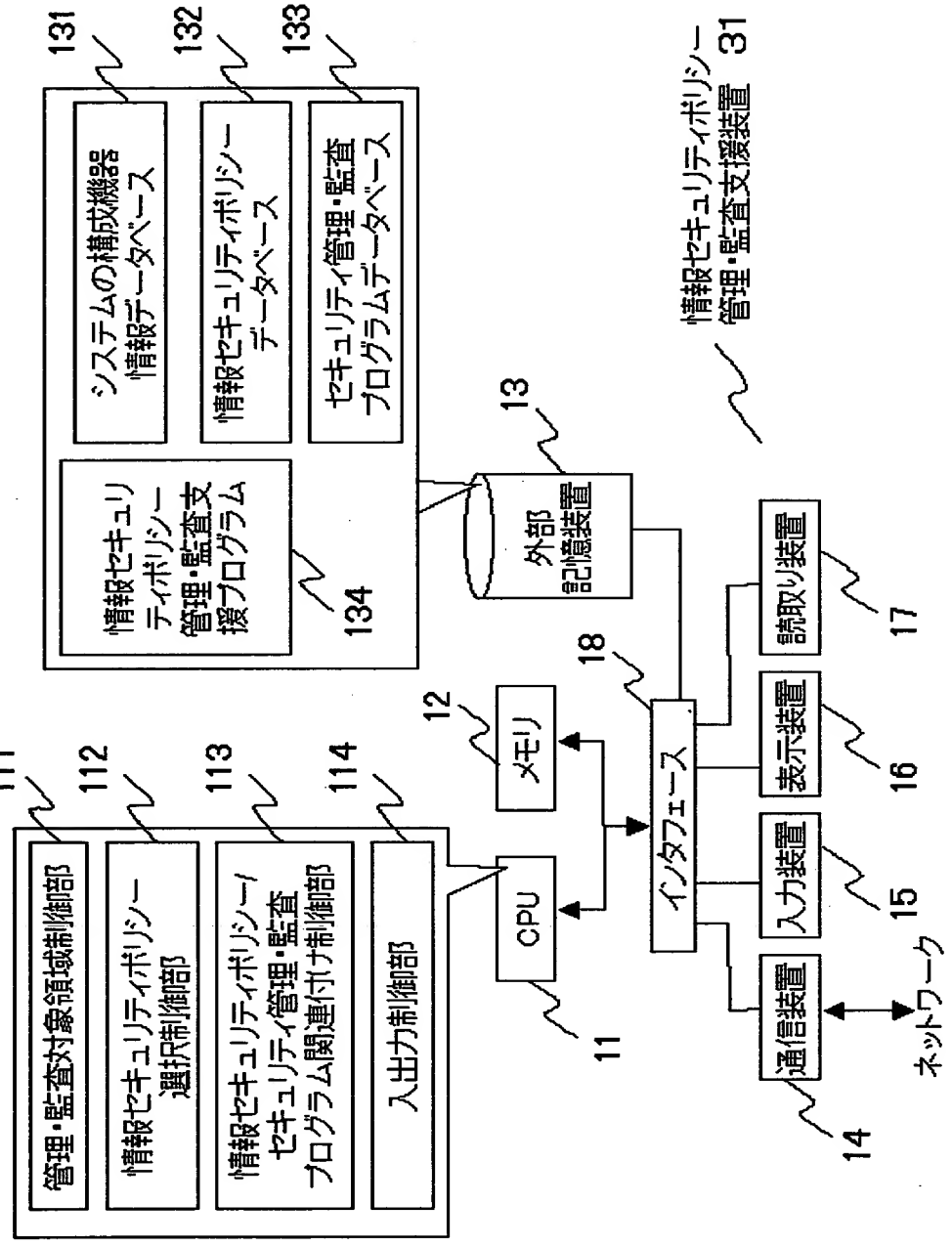
図1



出証特２００１－３００８３９７

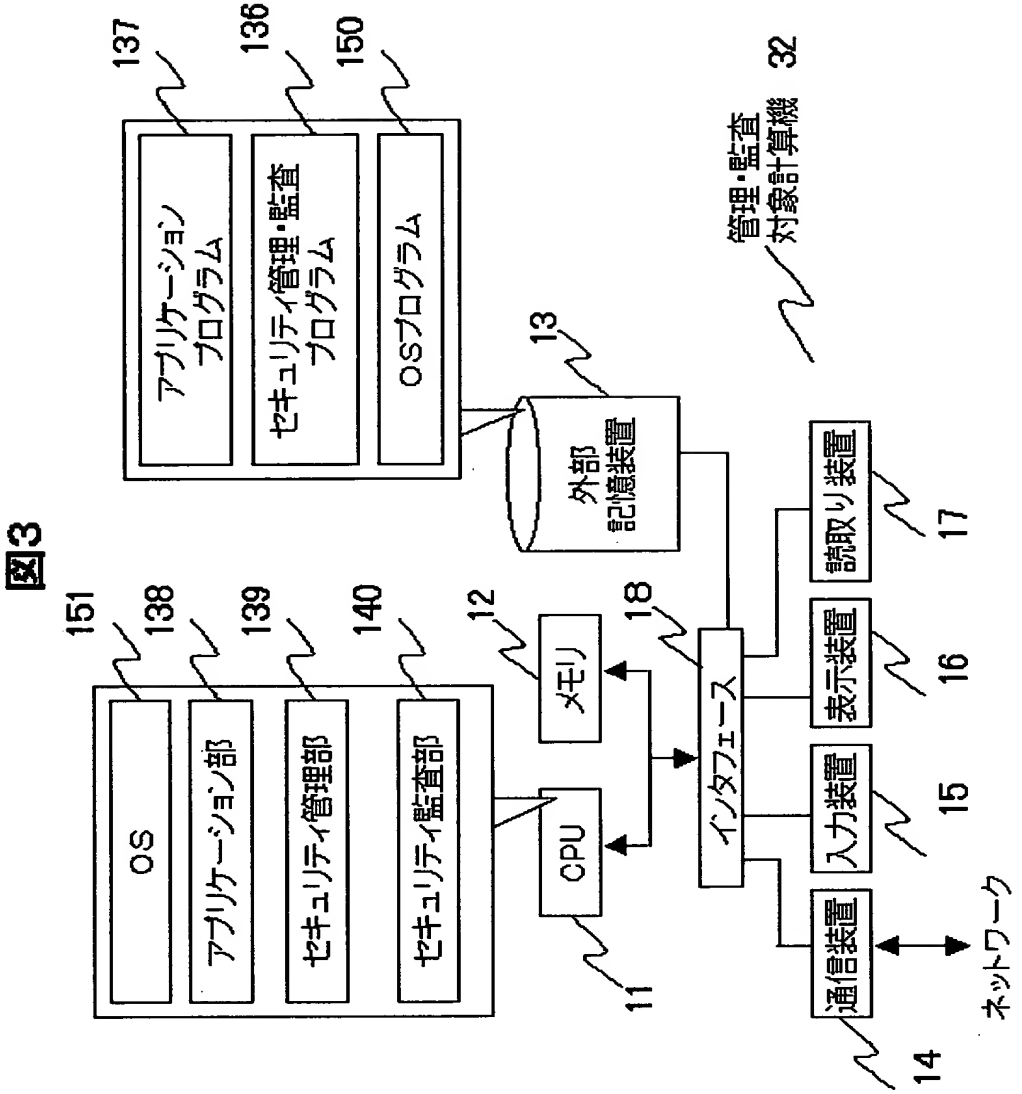
【図２】

図2


131
132
133
システムの構成機器
情報データベース
情報セキュリティポリシー
データベース
セキュリティ管理・監査
プログラムデータベース
情報セキュリティポリシー
管理・監査支援プログラム
134
13
外部
記憶装置
情報セキュリティポリシー
管理・監査支援装置
31
111
112
113
114
管理・監査対象領域制御部
情報セキュリティポリシー
選択制御部
情報セキュリティポリシー
セキュリティ管理・監査
プログラム関連付け制御部
入出力制御部
12
メモリ
CPU
11
18
インタフェース
読取り装置
17
表示装置
16
入力装置
15
通信装置
14
ネットワーク

【図３】

図3


137
136
150
アプリケーション
プログラム
セキュリティ管理・監査
プログラム
OSプログラム
32
管理・監査
対象計算機
13
外部
記憶装置
151
138
139
140
12
18
OS
アプリケーション部
セキュリティ管理部
セキュリティ監査部
メモリ
インタフェース
読取り装置
17
表示装置
16
CPU
入力装置
15
11
通信装置
14
ネットワーク

【図４】

図4

41 SYSID	42 装置種別	43 ソフトウェア種別	44 プログラム名	45 選択可否
R001-00-01	ルータ	－	A	YES
R001-00-02			B	NO
： ：	： ：	： ：	： ：	： ：
S001-OS-01	サーバ	OS	H	YES
S001-OS-02			I	NO
S001-WEB-01		Web	X	YES
S001-WEB-02			Y	NO
S001-WEB-03			Z	NO
S001-MAIL-01		メール	O	YES
S001-DB-01		データベース	P	YES
： ：	： ：	： ：	： ：	： ：

【図５】

図5

51 POLICYID	52 施策種別	53 セキュリティ施策	54 選択可否
AUTH-01	識別と認証機能	ネットワークにアクセス可能な端末の限定	YES
AUTH-02	識別と認証機能	識別・認証情報用の良いパスワード設定の実施	YES
： ：	： ：	： ：	： ：
ACC-01	アクセス制御機能	端末やユーザ毎に利用可能なコマンドの限定	YES
ACC-02	アクセス制御機能	権限の設定・変更・削除可能者の限定	YES
ACCADM-01	アクセス監視	データ・プログラムの改ざん検出の実施	YES
ACCADM-02	アクセス監視	ユーザ使用コマンドの記録	NO
ACCADM-03	アクセス監視	アクセスログの取得	NO
VIRUS-01	ウィルス対策	ワクチンソフトウェアのインストール	
VIRUS-02	ウィルス対策	定期的なウィルスチェック	YES
VIRUS-03	ウィルス対策	定期的なウイルス定義データの更新	YES
： ：	： ：	： ：	： ：

【図６】

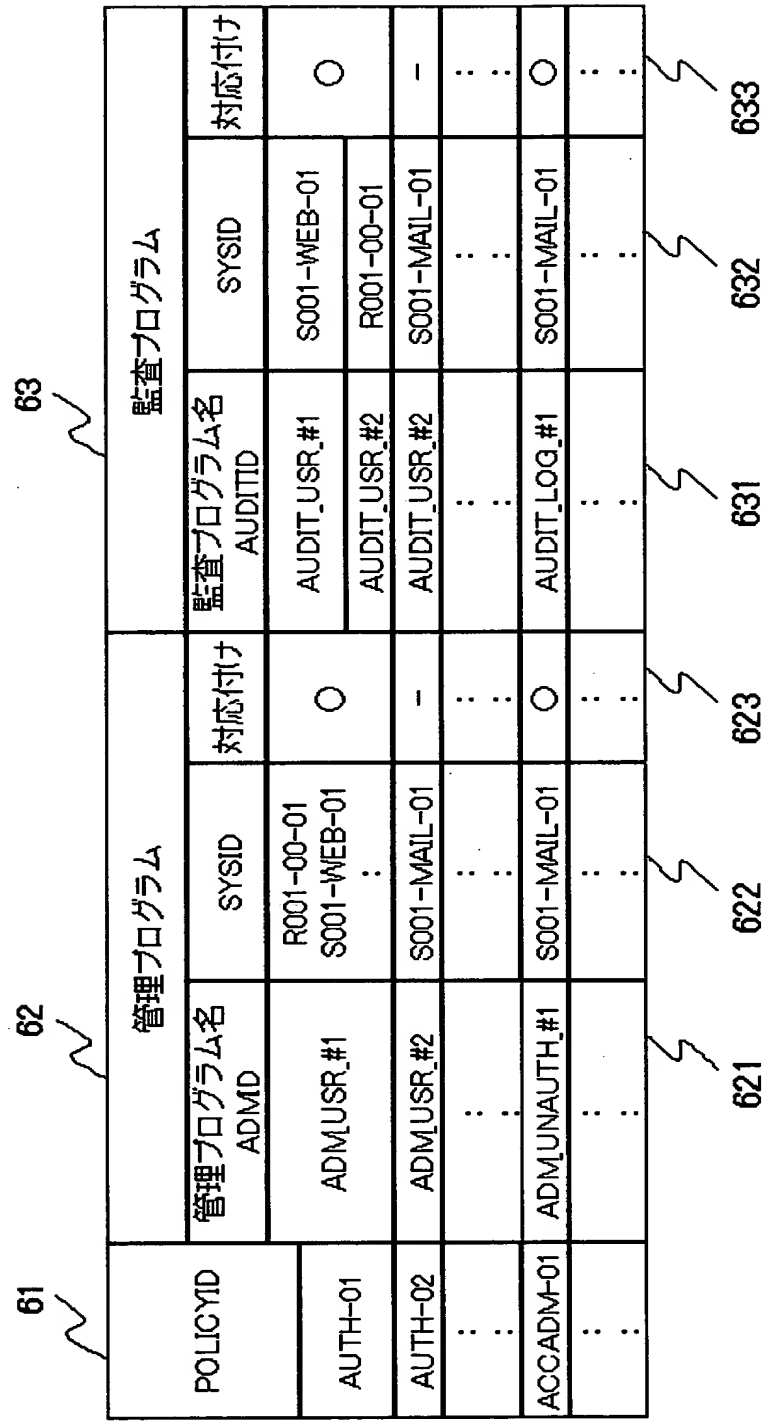
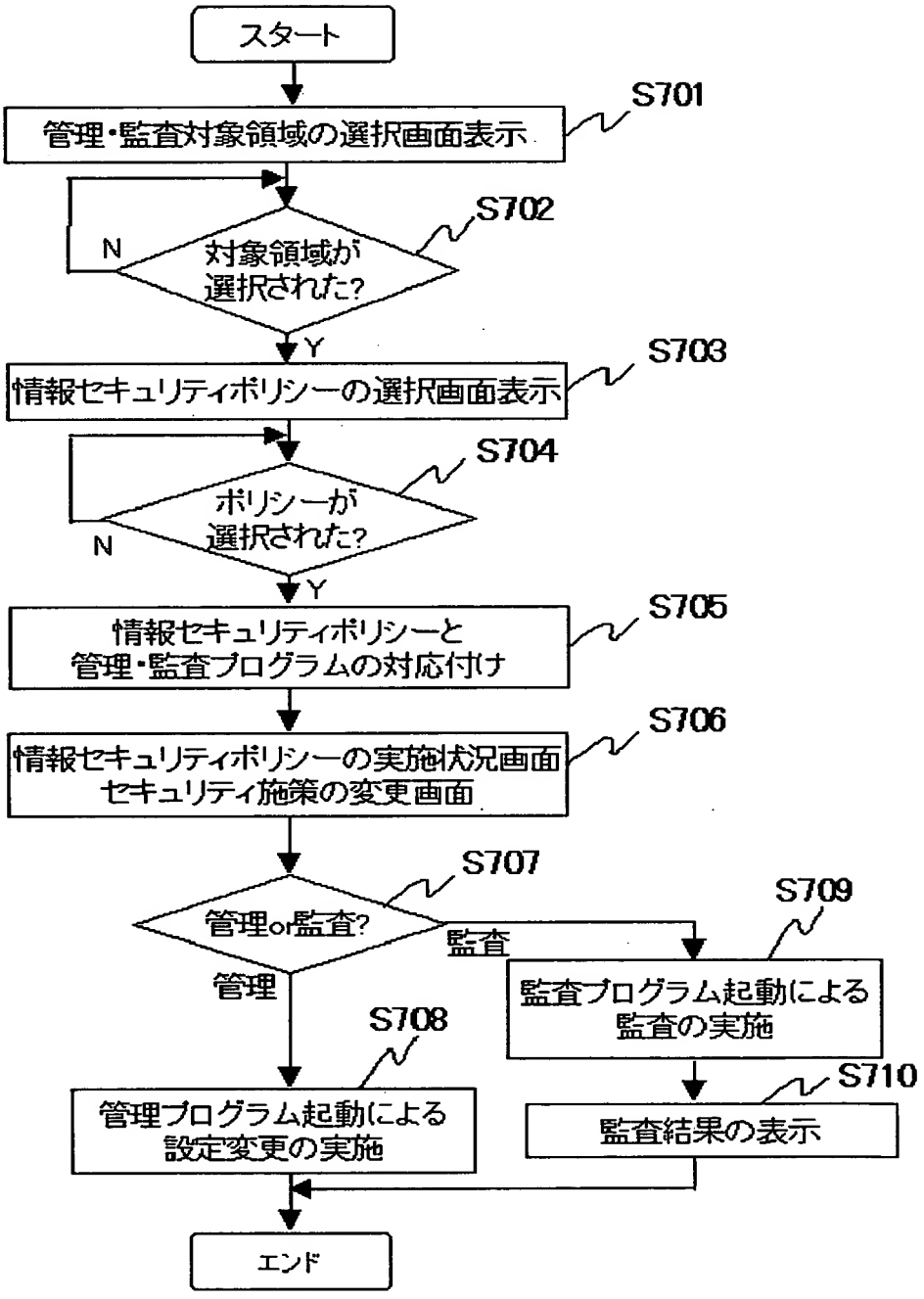


図6

POLICYID	管理プログラム			監査プログラム		
	管理プログラム名 ADMID	SYSID	対応付け	監査プログラム名 AUDITID	SYSID	対応付け
AUTH-01	ADM_USR_#1	R001-00-01 S001-WEB-01 :	○	AUDIT_USR_#1	S001-WEB-01	○
				AUDIT_USR_#2	R001-00-01	
AUTH-02	ADM_USR_#2	S001-MAIL-01	-	AUDIT_USR_#2	S001-MAIL-01	-
: :	: :	: :	: :	: :	: :	: :
ACCADM-01	ADM_UNAUTH_#1	S001-MAIL-01	○	AUDIT_LOG_#1	S001-MAIL-01	○
: :	: :	: :	: :	: :	: :	: :

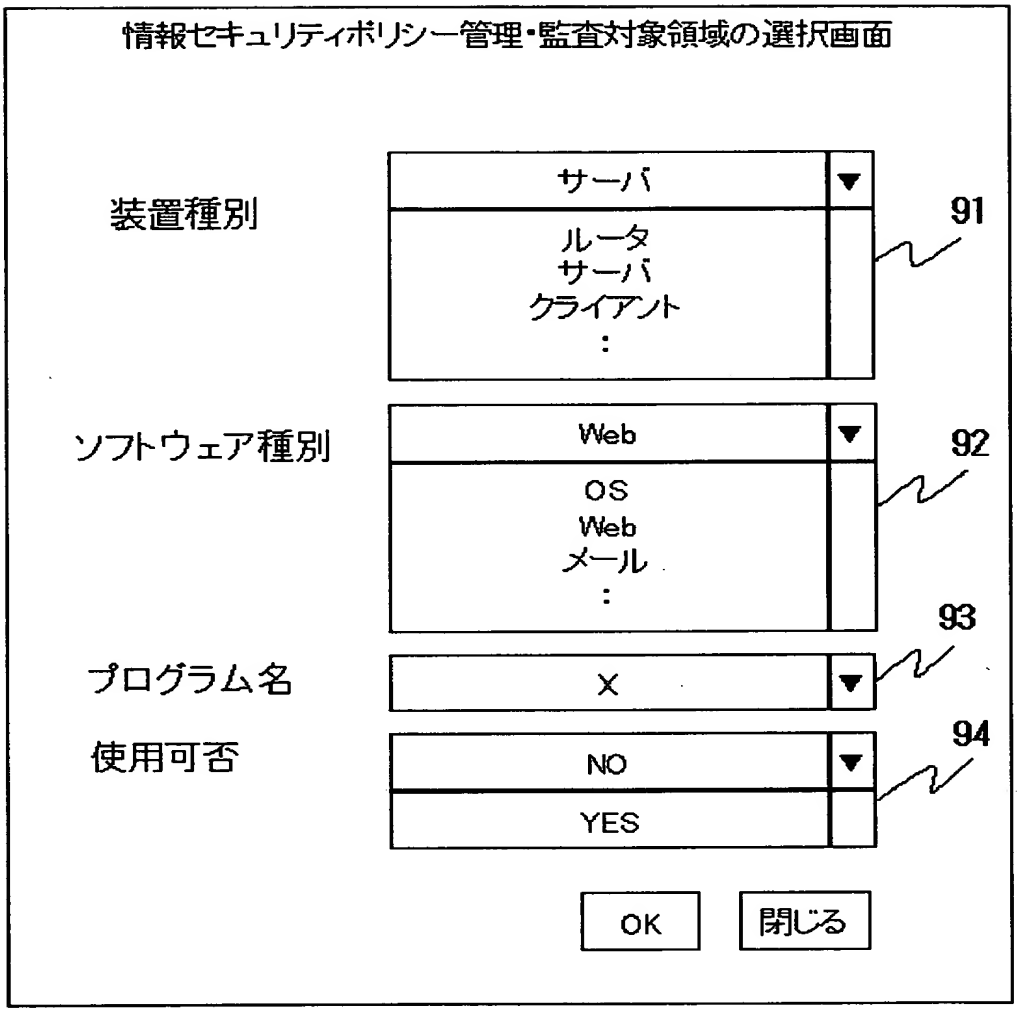
【図７】

図7


スタート
S701
管理・監査対象領域の選択画面表示
S702
N
対象領域が
選択された?
Y
S703
情報セキュリティポリシーの選択画面表示
S704
ポリシーが
選択された?
N
Y
S705
情報セキュリティポリシーと
管理・監査プログラムの対応付け
S706
情報セキュリティポリシーの実施状況画面
セキュリティ施策の変更画面
S707
管理or監査?
監査
S709
監査プログラム起動による
監査の実施
管理
S708
管理プログラム起動による
設定変更の実施
S710
監査結果の表示
エンド

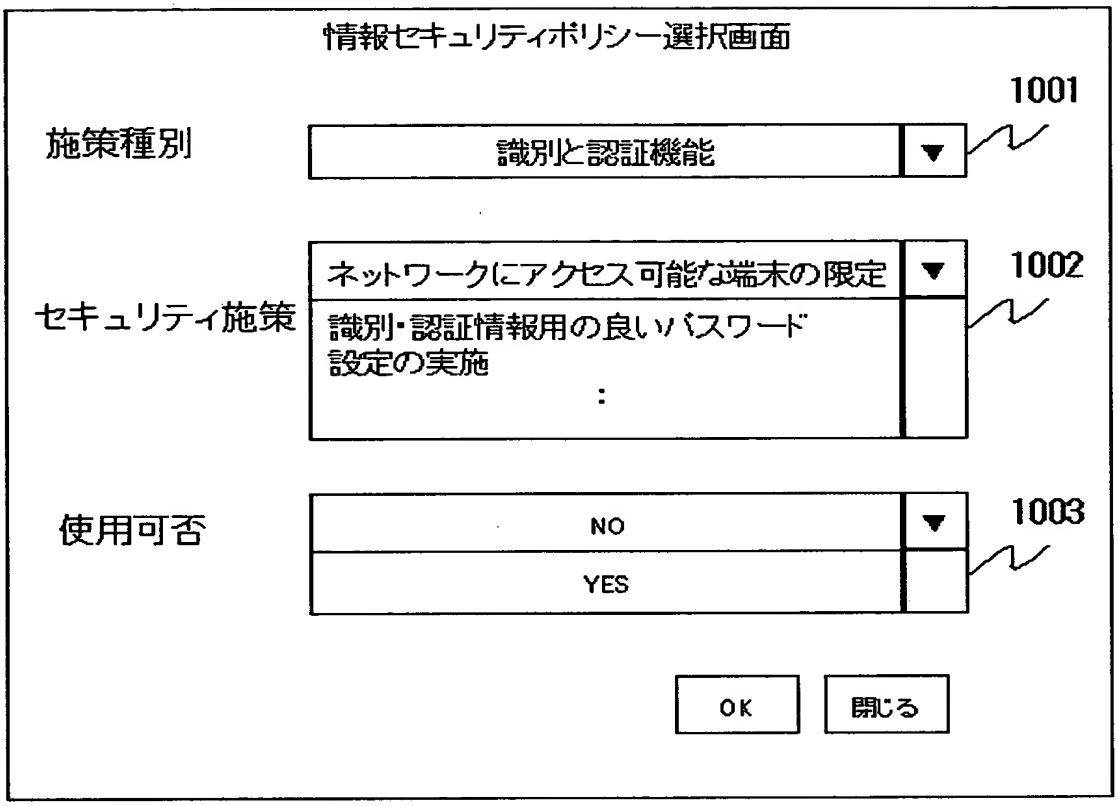
【図８】

図8


情報セキュリティポリシー管理・監査対象領域の選択画面
装置種別
サーバ
ルータ
サーバ
クライアント
:
91
ソフトウェア種別
Web
OS
Web
メール
:
92
プログラム名
X
93
使用可否
NO
YES
94
OK
閉じる

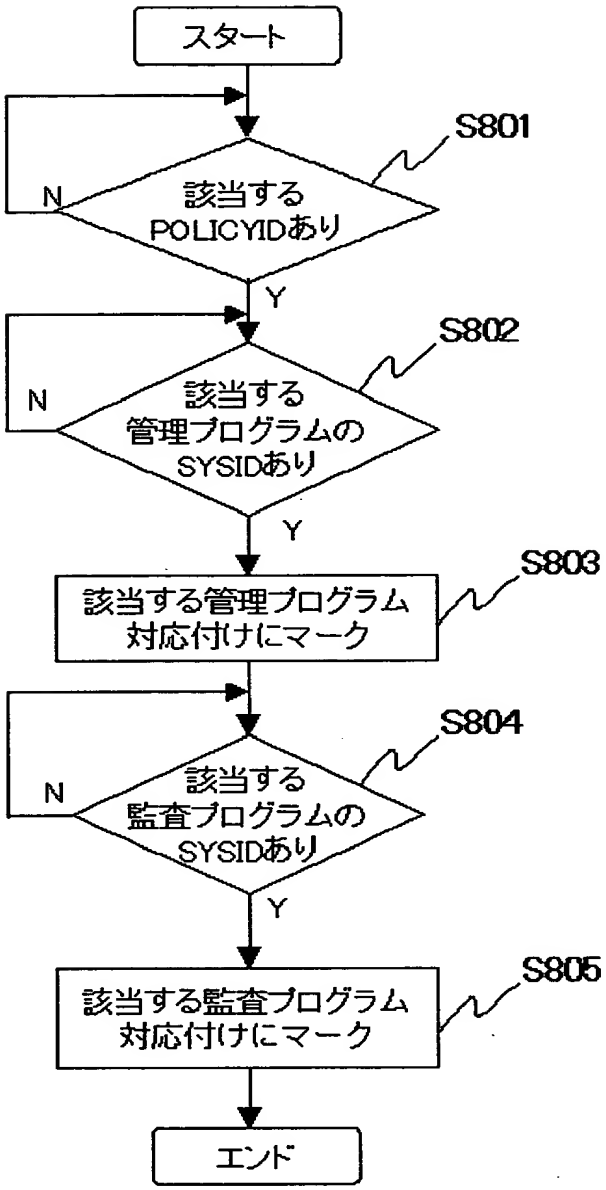
【図９】

図9


情報セキュリティポリシー選択画面
1001
施策種別
識別と認証機能
1002
セキュリティ施策
ネットワークにアクセス可能な端末の限定
識別・認証情報用の良いパスワード
設定の実施
:
1003
使用可否
NO
YES
OK
閉じる

【図１０】

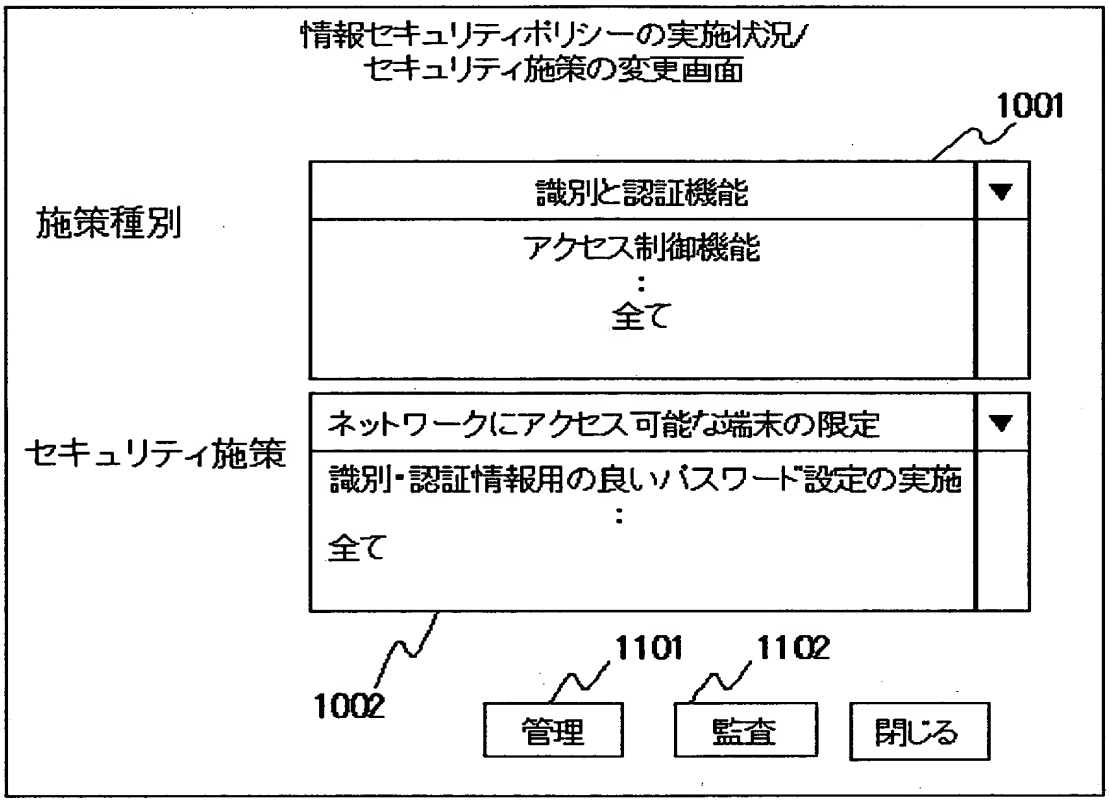
図10



出証特２００１－３００８３９７

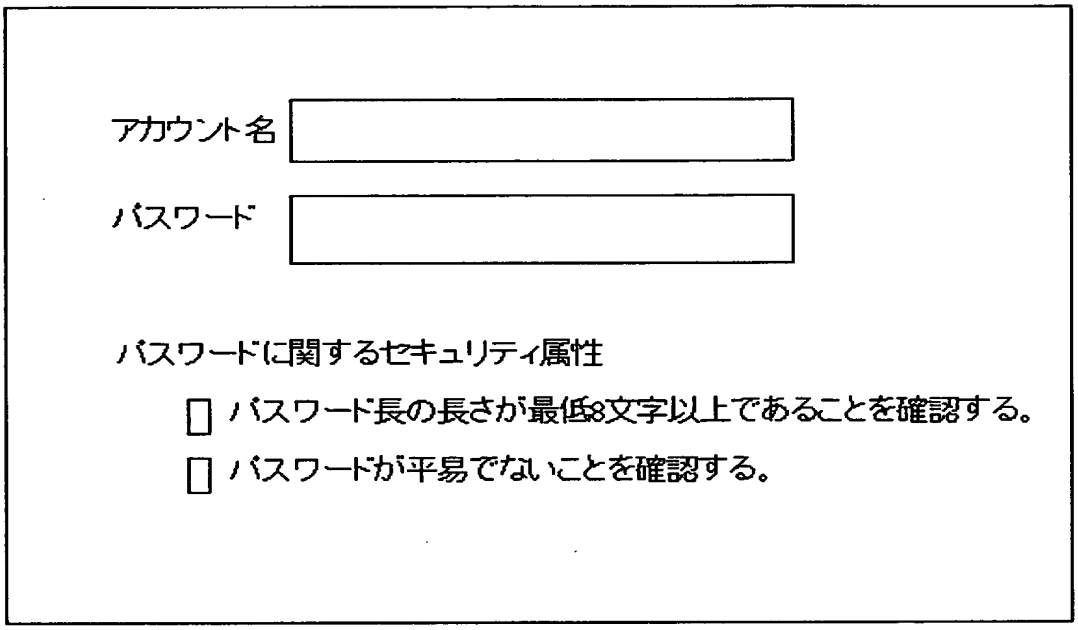
【図１１】

図11


情報セキュリティポリシーの実施状況/
セキュリティ施策の変更画面
1001
施策種別
識別と認証機能
アクセス制御機能
：
全て
セキュリティ施策
ネットワークにアクセス可能な端末の限定
識別・認証情報用の良いパスワード設定の実施
：
全て
1002
1101
1102
管理
監査
閉じる

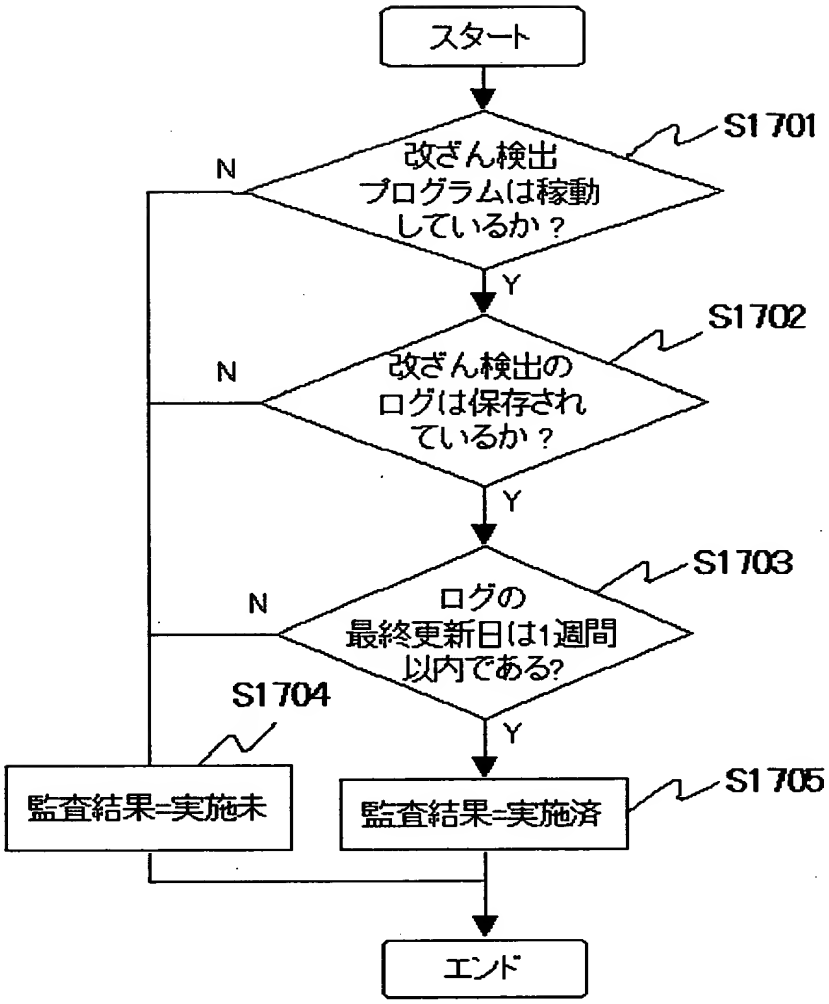
【図１２】

図12


アカウント名
パスワード
パスワードに関するセキュリティ属性
パスワード長の長さが最低8文字以上であることを確認する。
パスワードが平易でないことを確認する。

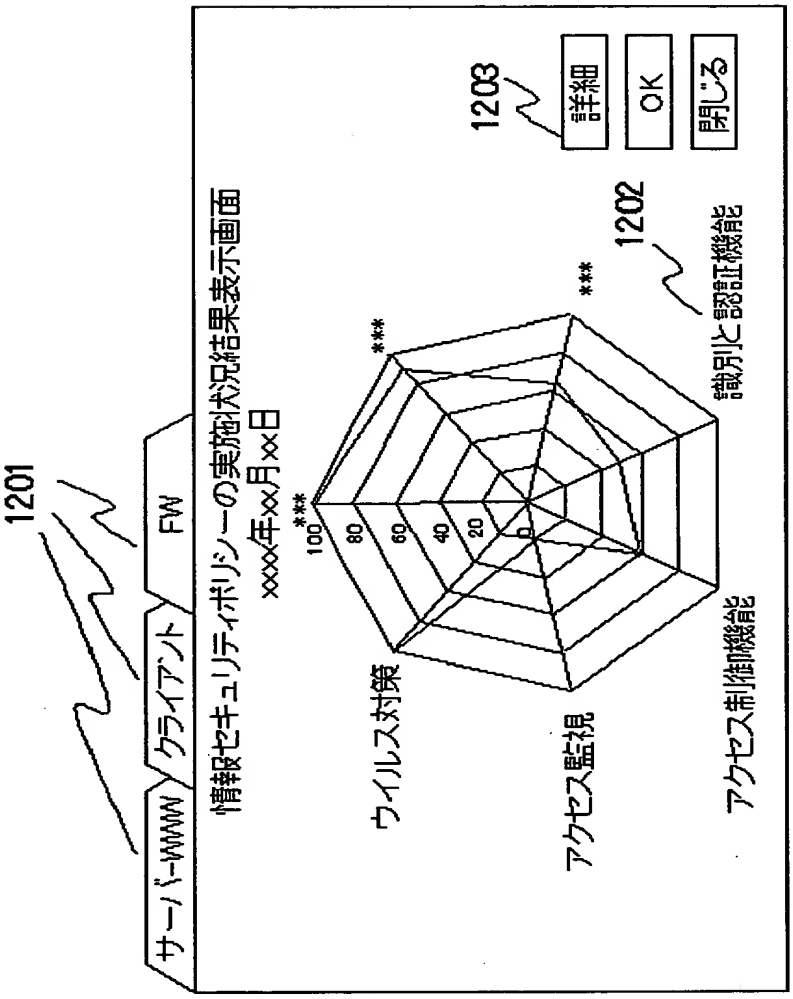
【図１３】

図13


スタート
S1701
改ざん検出
プログラムは稼動
しているか？
N
Y
S1702
改ざん検出の
ログは保存され
ているか？
N
Y
S1703
ログの
最終更新日は1週間
以内である?
N
Y
S1704
監査結果=実施未
S1705
監査結果=実施済
エンド

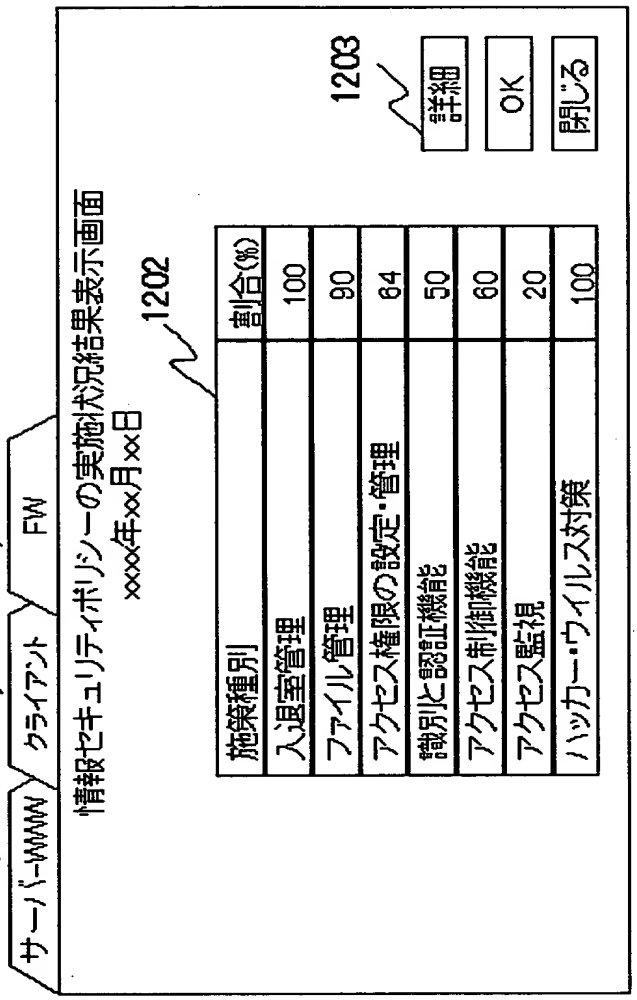
【図１４】

図14


1201
サーバ-WWW
クライアント
FW
情報セキュリティポリシーの実施状況結果表示画面
xxxx年xx月xx日
100
80
60
40
20
0
***
***
***
ウイルス対策
アクセス監視
アクセス制御機能
識別と認証機能
1202
1203
詳細
OK
閉じる

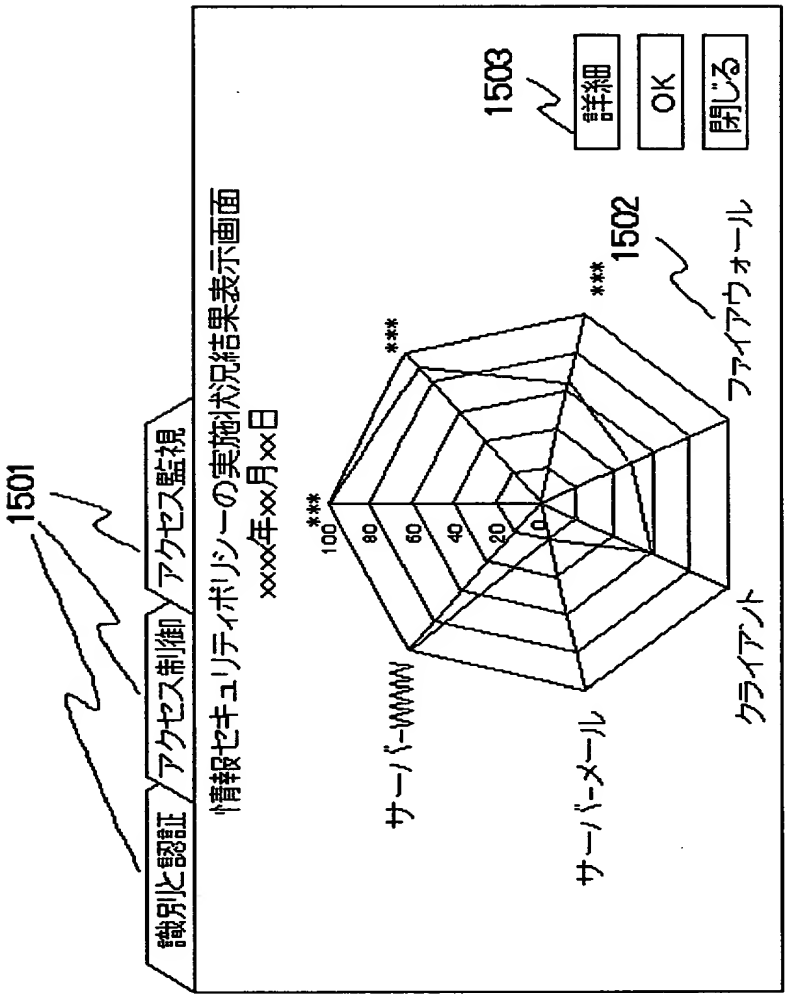
【図１５】

図15


1201
サーバ-WWW
クライアント
FW
情報セキュリティポリシーの実施状況結果表示画面
××××年××月××日
1202
施策種別
割合(%)
入退室管理
100
ファイル管理
90
アクセス権限の設定・管理
64
識別と認証機能
50
アクセス制御機能
60
アクセス監視
20
ハッカー・ウィルス対策
100
1203
詳細
OK
閉じる

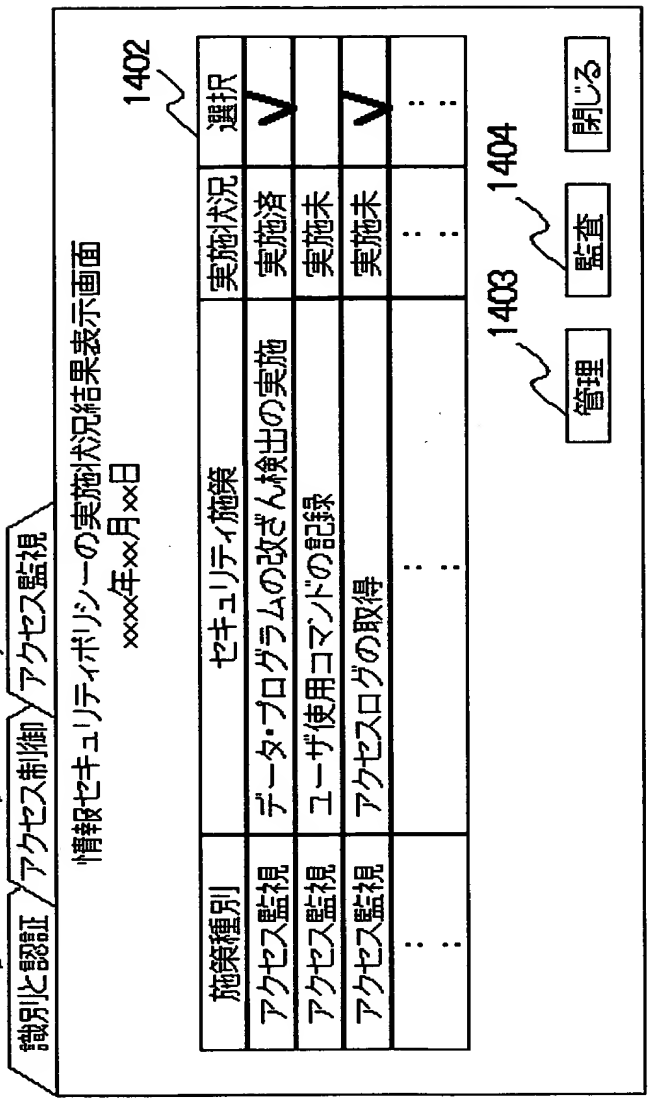
【図１６】

図16


1501
識別と認証
アクセス制御
アクセス監視
情報セキュリティポリシーの実施状況結果表示画面
××××年××月××日
100
80
60
40
20
0
***
***
***
1502
サーバ-WWW
サーバ-メール
ファイアウォール
クライアント
1503
詳細
OK
閉じる

【図１７】

図17


1401
識別と認証
アクセス制御
アクセス監視
情報セキュリティポリシーの実施状況結果表示画面
××××年××月××日
1402
施策種別
セキュリティ施策
実施状況
選択
アクセス監視
データ・プログラムの改ざん検出の実施
実施済
アクセス監視
ユーザ使用コマンドの記録
実施未
アクセス監視
アクセスログの取得
実施未
1403
1404
管理
監査
閉じる

【書類名】　要約書

【要約】

【課題】情報セキュリティポリシーに従った企業情報システムのセキュリティ管理・監査を簡単にする。

【解決手段】情報セキュリティポリシーおよび対象システムと管理・監査プログラムを対応づけたセキュリティー管理・監査プログラムデータベース133を設ける。操作者により指定された情報セキュリティポリシーおよび対象システムの範囲に対応する管理・監査プログラムを検索し、自動的に実行する。管理・監査プログラムは、自身に対応する対象システムの情報セキュリティポリシーに関する管理・監査を行う。

【選択図】図２

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所